

Weekly Report

2019.06.03-2019.06.09

Doing & done

Mon, 8h

文献阅读

- ☒ 阅读《Practical Secure Aggregation for Privacy-Preserving Machine Learning》第一部分

投稿

- ☒ 和林昊、雅博讨论下来打算以：联邦学习过程中，共享权重的边缘处理、加密传输等步骤的隐私保护效果为切入口。例如以模拟攻击、信息熵变化等方式进行可视化。（林昊的想法是基于权重向量对参与训练的client进行聚类，基于交互做一些实时监测分析。应该重点挺不一样的）

Tue, 8h

投稿

- ☒ 准备idea的PPT

《计算机网络》课程作业

- ☒ 论文&展示：区块链技术原理和相关产品

Wed, 8h

在玉泉上课

- ☒ 《高级操作系统》

准备0614组会报告

- ☒ 查找并确定报告文献为《Narvis: Authoring Narrative Slideshows for Introducing Data Visualization Designs》，阅读了前半部分。

Thu, 8h

tensorflow_federated colab document

- ☒ "In order to facilitate experimentation, we seeded the TFF repository with a few datasets, including a federated version of MNIST that contains a version of the original NIST dataset that has been re-processed using Leaf so that the data is keyed by the original writer of the digits. Since each writer has a unique style, this dataset exhibits the kind of non-i.i.d. behavior expected of federated datasets."

tensorflow_federate 中demo的做法刚好验证了我之前的想法，证明了可行性。

在玉泉上课

☑ 《计算机网络》

Fri, 8h

神经网络的可解释性

- ☑ 查找并阅读相关文献。现有的大部分工作是针对神经网络的一些特定结构如CNN和RNN等可视化进行“黑箱理解”。对特定问题能起到较好的效果，但是似乎对神经网络不具有普适性，例如全连接层的参数如何理解实际含义？这是一个很基础的问题。不过，其中一个令我受到启发的做法是对在CNN可视化时，对其中的池化层提出的反池化操作。从而使得对某个中间步骤的抽象数据进行了可视化还原。这种“反计算”思维似乎对加密数据的可视化工作有一定借鉴意义。

Work plan

- 认真准备并完成组会报告的PPT。
- 配置环境，运行tff的demo，验证这周提出的初步想法。思考如何对用户的参数特征数据进行挖掘。
- 继续阅读同态加密相关算法、深度学习可解释性、隐私保护机器学习相关论文。